Mandate of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

REFERENCE:
OL AUS 5/2018

11 September 2018

Excellency,

I have the honour to address you in my capacity as Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 34/18.

In this connection, I would like to submit the following comments on the **Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018** ("the draft Bill"), in response to the call for comments by the Department of Home Affairs ("the Department").

According to the information received:

The Department of Home Affairs published the draft Bill on 14 August 2018. While the Bill acknowledges that encryption is a critical digital security measure, it also expresses the concern that encryption is being "employed by terrorists, child sex offenders and criminal organisations to mask illegal conduct."[1] The 176-page draft Bill is "intended to secure critical assistance from the communications industry and enable law enforcement to effectively investigate serious crimes in the digital era."[2] In a bid to ensure that the draft Bill is a "necessary and proportionate response" to illicit uses of encryption, the Department has solicited comments from the public. The deadline for comments is 10 September 2018.[3]

As a threshold matter, given the seriousness of the issues being considered and the length and complexity of the draft Bill, **I urge your Excellency's Government to extend the deadline for comments.**

I also wish to bring to the attention of the Department some of the provisions of the draft Bill that, if adopted, would severely impinge on the rights to privacy and freedom of expression and association, as provided by articles 17 and 19 of the International Covenant on Civil and Political Rights ("the Covenant"), ratified by Australia on 13 August 1980. I recall that these rights can only be subject to restrictions in strictly defined circumstances, when provided by the law and if abiding the strict requirements of necessity and proportionality.

---

1 https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018
2 *Id.*
3 *Id.*

I am concerned that the draft Bill is inconsistent with Australia's obligations under Article 17 and 19 of the Covenant. I am particularly concerned that the draft Bill gives virtually unfettered discretion to agencies to compel providers to modify digital security standards or take other action that would effectively weaken encryption. I urge the Department to reconsider the draft Bill in line with the human rights standards outlined below, as well as my recommendations based on these standards.

A. International human rights framework for assessing the draft Bill's compliance with the right to information and freedom of expression

Before explaining my specific concerns with the draft Bill, I wish to remind your government of its obligations under articles 17 and 19 of the International Covenant on Civil and Political Rights ("the Covenant"), ratified by Australia on 13 August 1980.

Article 19(1) of the Covenant establishes the right to freedom of opinion without interference. Article 19(2) establishes State Parties' obligations to respect and ensure "the right to freedom of expression," which includes the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." Whereas article 19(3) provides that restrictions on the right to freedom of expression must be "provided by law", and necessary "for respect of the rights or reputations of others" or "for the protection of national security or of public order (ordre public), or of public health and morals." Permissible restrictions on the internet are the same as those offline.[4]

Since article 19(2) "promotes so clearly a right to information of all kinds," this indicates that "States bear the burden of justifying any withholding of information as an exception to that right."[5] The Human Rights Committee, the body charged with monitoring implementation of the Covenant, has also emphasized that limitations should be applied strictly so that they do "not put in jeopardy the right itself."[6]

Under the article 19(3) requirement of legality, it is not enough that restrictions on the right to information are formally enacted as domestic laws or regulations. Instead, restrictions must also be sufficiently clear, accessible, and predictable.[7]

The requirement of necessity also implies an assessment of the proportionality of restrictions, with the aim of ensuring that restrictions "target a specific objective and do

---

4 Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue, A/HRC/17/27, ¶ 69, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

5 General Assembly, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/70/361, ¶ 8 ("A/70/361"), available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361.

6 U.N. Human Rights Comm., General Comment No. 34, article 19: Freedoms of opinion and expression, U.N. Doc. CCPR/C/GC/34, ¶21 (September 12, 2011) ("General Comment 34"), available at http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

7 *Id.* ¶ 25.

not unduly intrude upon the rights of targeted persons."[8] The ensuing interference with third parties' rights must also be limited and justified in the interest supported by the intrusion.[9] Finally, the restrictions must be "the least intrusive instrument among those which might achieve the desired result."[10]

Although article 19(3) recognizes "national security" as a legitimate aim, the Human Rights Council has stressed "the need to ensure that invocation of national security, including counter-terrorism, is not used unjustifiably or arbitrarily to restrict the right to freedom of opinion and expression."[11] In this regard, I have concluded, in my capacity as Special Rapporteur, that national security considerations should be "limited in application to situations in which the interest of the whole nation is at stake, which would thereby exclude restrictions in the sole interest of a Government, regime, or power group."[12] Additionally, States should "demonstrate the risk that specific expression poses to a definite interest in national security or public order, that the measure chosen complies with necessity and proportionality and is the least restrictive means to protect the interest, and that any restriction is subject to independent oversight."[13]

Article 17 of the Covenant specifically protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and "unlawful attacks on his or her honour and reputation," and provides that "everyone has the right to the protection of the law against such interference or attacks." The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression.[14]

Encryption and anonymity are protected because they play a critical role in securing both the right to privacy and the right to freedom of expression.[15] "Encryption provides security so that individuals are able 'to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion.'"[16] Accordingly, laws

---

8 Human Rights Council, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/29/32, ¶ 35 ("A/HRC/29/32"); *see also* U.N. Human Rights Comm., General Comment No. 27, Freedom of movement (Art. 12), U.N. Doc. CCPR/C/21/Rev.1/Add.9 (Nov 2, 1999) ("General Comment 27"),available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2f21%2fRev.1%2fAdd.9&Lang=en.

9 *Id.*

10 General Comment 27, *supra* n. 5, at ¶14.

11 Human Rights Council, U.N. Doc. A/HRC/7/36 (Mar. 28, 2008), *available at* http://ap.ohchr.org/documents/E/HRC/resolutions/A_HRC_RES_7_36.pdf.

12 General Assembly, Report of the Spec. Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/71/373, ¶18, *available at* https://undocs.org/A/71/373.

13 *Id.*

14 General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8.

15 A/HRC/23/40 and Corr.1.

16 A/HRC/29/32, supra note 8, (quoting A/HRC/23/40 and Corr.1).

addressing encryption must comply with the requirements of legality, necessity and proportionality established under international human rights law.[17] In the May 2015 report, submitted in accordance with Human Rights Council resolution 25/2, I addressed the use of encryption and anonymity in digital communications:

> "First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation. . . .[18] Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. . . . Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective.[19]"

The Special Rapporteur found that "the regulation of encryption often fails to meet freedom of expression standards in two leading respects": (1) they are generally unnecessary to meet legitimate interest and (2) "they disproportionately impact the rights to freedom of opinion and expression enjoyed by targeted persons or the general population."[20]

B. Concerns regarding new compulsory and voluntary orders under the draft Bill

In light of these standards, the following provisions of the draft Bill raise concerns under the Covenant:

Section 317G would allow the Director-General of Security, the Director-General of the Australian Intelligence Service, the Director General of the Australian Signals Directorate or the chief officer of an interception agency to make a "technical assistance request" that "may ask the [designated communications] provider to do acts or things on a voluntary basis that are directed towards ensuring that the provider is capable of giving certain types of help" to law enforcement, Under Section 317G(6), the technical assistance request allows the Government to ask the provider for information " in connection with any or all of the eligible activities of the provider."

Section 317L would authorize the Director-General of Security of the chief officer of an interception agency to issue a "technical assistance notice that requires [or compels] the provider to do acts or things by way of giving help" to law enforcement. Section 317L also specifies that a technical assistance notice can be given if it relates to various power and functions, including enforcing the criminal law and laws imposing pecuniary penalties; assisting the enforcement of the criminal laws in force in a foreign country; or protecting the public revenue; or safeguarding national security; or a matter that facilitates, or is ancillary or incidental to any of the above powers and functions. Section

---

[17] *Id.*

[18] *See* Human Rights Committee, general comment No. 34 (2011)

[19] Human Rights Committee, general comment No. 34, para. 2, and communication No. 2156/2012, Views adopted on 10 October 2014

[20] A/HRC/29/32, supra note 8.

317P provides that the government cannot give a technical assistance notice unless it is satisfied that the requirements imposed by the notice are reasonable and proportionate.

Section 317T would allow the Attorney-General, in accordance with a request made by the Director-General of Security or the chief officer of an interception agency, to give a provider a written "technical capability notice [that] may require the provider to do acts or things directed towards ensuring that the provider is capable of giving certain types of help." Such a notice must be for the purposes of enforcing the criminal law and laws imposing pecuniary penalties; assisting the enforcement of the criminal laws in force in a foreign country; protecting the public revenue; or safeguarding national security. Similar to a technical assistance notice, the Attorney-General must not give a technical capability notice to a designated communications provider unless the Attorney-General is satisfied that the requirements imposed by the notice are reasonable and proportionate.

Section 317E provides a non-exhaustive list of examples regarding what "help" organizations can be ordered to do or what providers can be compelled to have the capabilities to do with respect to "technical assistance requests" and "technical assistance notice," including "removing one or more forms of electronic protection; providing technical information; installing, maintaining, testing or using software or equipment;" and providing physical access to infrastructure.

Based on my understanding of the text of the draft Bill and how it would relate to pre-existing laws, policies, and regulations Schedule 1, Section 317, would have the following practical implications:

> Companies would be asked to voluntarily, and non-voluntarily, disclose information about how their networks are built and how they store their information;
>
> Companies would be ordered to comply with law enforcement agencies or ensure that the have the capability to comply with Government requests;
>
> Agencies would specify removing electronic protection, and could require the provider to build a capability to remove electronic protection, which includes decrypting encrypted communications; and
>
> Companies could be compelled to disclose "formation about the design, manufacture, creation or operation of a service, the characteristics of a device, or matters relevant to the sending, transmission, receipt, storage or intelligibility of a communication."[21]

[21] Explanatory Document of the Access and Assistance Bill, 26, https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf.

As described below, the three types of assistance place unnecessary mandates on companies, infringing on the zone of privacy created by encryption and anonymity to protect freedom of expression, conflicting with articles 19 and 17 of the Covenant.[22]

The limitations on compulsory and voluntary orders are vague and ambiguous

Section 317ZG, provides limitations restricting what the Government and agencies can require of the providers, specifically "[a] technical assistance notice or technical capability notice must not have the effect of: (a) requiring a designated communications provider to implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection." The Explanatory Document accompanying the draft Bill ensures that "providers **cannot** be asked to implement or build so-called 'backdoors' into their products or services."

While the Explanatory Document explicitly states that a "backdoor" is not being created, the ambiguity in Section 317ZG raise concerns that a keyed backdoor or access to a "front door" is being created. Thus, this Section still provides for measures that in practice could systematically weaken encryption and digital security. Neither Section 317ZG or the Explanatory Document provide a definition for "systematic weakness." The ambiguity in the limitation, and the lack of definition for "systemic weakness" raise concern that compulsory and voluntary orders are not in fact limited and unduly interfere with the right to privacy and the right to freedom of expression.

The draft Bill places inadequate limits on what the government can ask providers to do

The government can make requests or issue notices as long as the Attorney-General deems them to be reasonable and proportionate. Section 317E provides a list of examples regarding what "help" organizations can be ordered to do or what providers can be compelled to have the capabilities to do, but this list is non-exhaustive. The criteria for requests and notices are not only vaguely formulated, but also appear to be lower than the threshold of necessity, proportionality and legitimacy of objective envisioned under Article 19(3).

The decision-making criteria for "technical assistance notices" and "technical capability notices" raise concerns of unbounded discretion

It is important to note that the draft Bill does not create any warrant or oversight process regarding the issuance of these notices other than that they must be "reasonable and proportionate." Section 317V provides the same criteria for technical capability notices. The Explanatory Document suggests this includes balancing "the objectives of the agency, the availability of other means to reach those objectives, the likely benefits to an investigation and the likely business impact on the provider. . . wider public interests, such as any impact on privacy, cyber security and innocent third parties." Overall, the draft Bill provides the government with broad discretion to issue notices, and as

[22] A/HRC/29/32, *supra*.

explained above, the reasonableness standard does not meet the strict tests of necessity and proportionality under article 19(3) of the Covenant.

The draft Bill also does not mention the ability of providers to challenge notices in court. However, the Explanatory Document states: "Technical assistance notices and technical capability notices are not subject to merits review. As opposed to judicial review, which ensures that decisions were made within the legal limits of the relevant power, merits review aims to ensure the 'correct' decision is made."

The general lack of accountability and oversight in the draft Bill also raises concerns that the process is arbitrary and uncertain.

The civil and criminal penalties for providers are individuals raise concerns of proportionality

Section 317ZB applies civil penalty units to designated communication providers (other than carriers and carriage service providers) that fail to comply with a technical assistance notice or technical capability notice. The penalty for body corporates is 47,619 penalty units, approximately AUD $10 million. The penalty for non-compliance by persons who are not body-corporates is 238 penalty units, approximately AUD $50,000. The large amount of money fined on those who fail to comply with the law, coupled with the unclear requirements raise heighten concerns that the punishment is disproportionate to the conduct.

C. Recommendations

In light of these concerns, and without prejudice to any other potential considerations related to the lengthy draft Bill, I urge the Department to consider the following recommendations in order to bring the draft Bill in line with human rights standards:

1. Technical assistance requests and technical assistance and capability notices should be subject to the authorization of an independent and impartial judicial body on a case-by-case basis. The judicial body should review the request or the notice to ensure that it meets the requirements of legality, necessity, proportionality and legitimacy of objective.

2. The draft Bill should specify that the relevant judicial body should authorize requests or notices only upon the government's showing of a real and identifiable risk of significant harm to a legitimate and specifically defined interest (such as national security or public order). The judicial body should also consider whether the government has exhausted all alternative technical and operational measures to conduct the investigation at issue.

3. The draft Bill should provide a clear and acceptably narrow definition of the term "systemic weakness." The definition should explicitly clarify that relevant authorities are not permitted to request or require private actors to facilitate backdoor access or intentionally weaken encryption and associated digital security measures in commercially available products and services.

4. The draft Bill should also prohibit requests or notices for assistance that would mandate local storage of all user data (including encryption keys) or the establishment of key escrows.

5. The draft Bill should reduce the civil penalties for non-compliance with technical assistance and capability notices.

6. While I commend the Department's call for public comments, I also urge meaningful and transparent consultations with a representative cross-section of civil society, corporations, the general public and other relevant stakeholders throughout the life cycle of the draft Bill.

Finally, I would like to inform you that this communication, as a comment on pending or recently adopted legislation, regulations or policies, will be made available to the public and posted on the website page for the mandate of the Special Rapporteur on the right to freedom of expression: http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/LegislationAndPolicy.aspx.

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression